

Comments on “A New Method to Compute the 2-Adic Complexity of Binary Sequences”

Honggang Hu

School of Information Science and Technology

University of Science and Technology of China

Hefei, China, 230027

Email. hghu2005@ustc.edu.cn

Abstract

We show that there is a very simple approach to determine the 2-adic complexity of periodic binary sequences with ideal two-level autocorrelation. This is the first main result by H. Xiong, L. Qu, and C. Li, IEEE Transactions on Information Theory, vol. 60, no. 4, pp. 2399-2406, Apr. 2014, and the main result by T. Tian and W. Qi, IEEE Transactions on Information Theory, vol. 56, no. 1, pp. 450-454, Jan. 2010.

1 A Very Simple Approach

Let $S = \{s_i\}_{i=0}^{+\infty}$ be a periodic binary sequence with period N , and $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$. Let us write

$$\frac{S(2)}{2^N - 1} = \frac{\sum_{i=0}^{N-1} s_i 2^i}{2^N - 1} = \frac{p}{q}$$

with $0 \leq p \leq q$, and $\gcd(p, q) = 1$.

Definition 1 ([3]) *With the notations as above, the 2-adic complexity $\Phi(S)$ of S is the real number $\log_2 q$.*

Remark 1 *If $\gcd(S(2), 2^N - 1) = 1$, then the 2-adic complexity $\Phi(S)$ of S achieves the maximum value $\log_2(2^N - 1)$.*

For any $0 \leq \tau < N$, the autocorrelation of S at shift τ is defined by

$$C_S(\tau) = \sum_{i=0}^{N-1} (-1)^{s_{i+\tau} + s_i}.$$

If $C_S(\tau) = -1$ for any $0 < \tau < N$, we call S an ideal two-level autocorrelation sequence [1]. There are three cases of N such that there exists an ideal two-level autocorrelation sequence of period N : 1) $N = 2^n - 1$; 2) $N = p$, where p is a prime number with $p \equiv 3 \pmod{4}$; 3) $N = p(p+2)$, where both p and $p+2$ are prime numbers [1].

Let $P(x) = \sum_{i=0}^{N-1} (-1)^{s_i} x^i \in \mathbb{Z}[x]$. If S is an ideal two-level autocorrelation sequence, then we have

$$\begin{aligned}
P(x)P(x^{-1}) &= \left(\sum_{i=0}^{N-1} (-1)^{s_i} x^i \right) \left(\sum_{j=0}^{N-1} (-1)^{s_j} x^{-j} \right) \pmod{x^N - 1} \\
&= \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (-1)^{s_i + s_j} x^{i-j} \pmod{x^N - 1} \\
&\equiv N + \sum_{\tau=1}^{N-1} \sum_{j=0}^{N-1} (-1)^{s_{j+\tau} + s_j} x^\tau \pmod{x^N - 1} \\
&\equiv N - x - x^2 - \dots - x^{N-1} \pmod{x^N - 1}.
\end{aligned}$$

As a consequence, we have

$$\begin{aligned}
P(2)P(2^{-1}) &\equiv N - 2 - 2^2 - \dots - 2^{N-1} \pmod{2^N - 1} \\
&\equiv N + 1 \pmod{2^N - 1}.
\end{aligned}$$

Note that $P(2) = \sum_{i=0}^{N-1} (-1)^{s_i} 2^i = \sum_{i=0}^{N-1} (1 - 2s_i) 2^i = 2^N - 1 - 2 \cdot S(2)$. Hence, we obtain the following interesting theorem.

Theorem 1 *With the notations as above, we have*

$$S(2)P(2^{-1}) \equiv -\frac{N+1}{2} \pmod{2^N - 1}.$$

By a simple argument, we can show that $\gcd(N+1, 2^N - 1) = 1$ as did in [5]. It follows that $\gcd(S(2), 2^N - 1) = 1$ which means that the 2-adic complexity of such sequences is maximum.

2 Conclusion

Using the property of ideal two-level autocorrelation carefully, we find a very simple way to show that the 2-adic complexity of ideal two-level autocorrelation sequences is maximum. This is the main result in [4], and the first main result in [5]. For the case of symmetric 2-adic complexity [2], the same result also holds as pointed out in [5].

References

- [1] S. Golomb and G. Gong, *Signal Designs With Good Correlation: For Wireless Communications, Cryptography and Radar Applications*. Cambridge, U.K.: Cambridge University Press, 2005.
- [2] H. Hu and D. Feng, "On the 2-adic complexity and the k -error 2-adic complexity of periodic binary sequences," *IEEE Trans. on Inform. Theory*, vol. 54, no. 2, pp. 874-883, Feb. 2008.
- [3] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," *J. Crypt.*, vol. 10, pp. 111-147, 1997.
- [4] T. Tian and W. Qi, "2-adic complexity of binary m -sequences," *IEEE Trans. on Inform. Theory*, vol. 56, no. 1, pp. 450-454, Jan. 2010.
- [5] H. Xiong, L. Qu, and C. Li, "A new method to compute the 2-adic complexity of binary sequences," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2399-2406, Apr. 2014.